

# CHECKLIST ISO/IEC 27001:2022

**Auditar un SGSI exige evidencias sólidas, no solo documentos.**

Este checklist de preparación ISO/IEC 27001:2022 te permitirá identificar el nivel de madurez de tu sistema, ordenar tus evidencias y planificar los siguientes pasos con claridad.



CERTIFICACIONES  
**CERTHIA**  
VALIDAMOS TUS PASOS

## Cómo usarlo

Marca cada ítem como  (listo),  (en progreso) o  (pendiente).

Añade evidencia (enlace/carpeta), responsable y fecha objetivo.

Puntuación orientativa: =2, =1, =0 (máx. 80).

- $\geq 64$ : base sólida; ajustar brechas y planificar auditoría.
- 48–63: priorizar brechas de evidencia y SoA; pre-assessment recomendado.
- $< 48$ : cerrar fundamentos (riesgos/SoA/operación) antes de agendar auditoría.

## A) Gobierno y alcance del SGSI

| Ítem                                                             | Qué tener                                                                                                                           | ✓ Listo | ⚠ En Progreso | ✗ Pendiente |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|---------|---------------|-------------|
| Alcance del SGSI definido (procesos, sedes, sistemas y terceros) | Documento de alcance con límites y exclusiones claras, mapa de procesos/sedes, tecnologías incluidas y terceros críticos.           |         |               |             |
| Política del SGSI aprobada, comunicada y vigente                 | Política firmada por dirección, fecha de revisión, difusión interna (intranet/inducción) y control de versiones.                    |         |               |             |
| Roles y responsabilidades formalizados (incl. responsable SGSI)  | Organigrama, RACI del SGSI, nombramiento del responsable, suplencias y criterios de competencia/formación.                          |         |               |             |
| Partes interesadas y requisitos aplicables identificados         | Listado de partes interesadas (clientes, reguladores, proveedores, personal) con sus requisitos legales/contractuales/regulatorios. |         |               |             |
| Control documental operativo (versionado, acceso, obsolescencia) | Procedimiento de control documental, repositorio único, permisos definidos, marca de "vigente/obsoleto" y trazabilidad de cambios.  |         |               |             |

Para más información contáctanos en nuestro sitio web **[www.certhia.pe](http://www.certhia.pe)**

## B) Riesgos y tratamiento

| Ítem                                                        | Qué tener                                                                                                                  | ✓ Listo | ⚠ En Progreso | ✗ Pendiente |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|---------|---------------|-------------|
| Metodología de análisis y evaluación de riesgos documentada | Método con criterios (probabilidad/impacto), fuentes (incidentes, vulnerabilidades, cambios), periodicidad y responsables. |         |               |             |
| Criterios de aceptación/apetito de riesgo definidos         | Umbral por criticidad, reglas de escalamiento y criterios para aceptar, mitigar, transferir o evitar riesgos.              |         |               |             |
| Registro de riesgos actualizado                             | Matriz con identificación, valoración, propietario, controles existentes y fecha de última actualización.                  |         |               |             |
| Plan de tratamiento aprobado (responsables y plazos)        | Acciones por riesgo, controles a implementar/ajustar, plazos, presupuestos cuando aplique y aprobaciones.                  |         |               |             |
| Seguimiento del plan de tratamiento (estado y evidencias)   | Tablero de ejecución, evidencia de cierres (tickets, PRs, actas) y revaloración del riesgo residual.                       |         |               |             |

Para más información contáctanos en nuestro sitio web **[www.certhia.pe](http://www.certhia.pe)**

## C) Declaración de Aplicabilidad (SoA)

| Ítem                                                      | Qué tener                                                                                                         | ✓ Listo | ⚠ En Progreso | ✗ Pendiente |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|---------|---------------|-------------|
| SoA alineada a 27001:2022 y 27002:2022                    | Listado de 93 controles por temas (organizacionales, personas, físico, tecnológico) con referencias actualizadas. |         |               |             |
| Controles justificados por riesgo (incluidas exclusiones) | Para cada control, motivo de inclusión; para exclusiones, razón objetiva ligada a alcance/escenario.              |         |               |             |
| Estado de cada control actualizado                        | Etiqueta por control (implantado / en progreso / no aplica) con fecha y próximo hito.                             |         |               |             |
| Evidencias y propietarios por control referenciados       | Enlace directo a evidencias (informes, tickets, logs) y rol responsable del control.                              |         |               |             |
| Métricas/criterios de eficacia definidos                  | 1-2 indicadores por control crítico (ej: % restauraciones exitosas; SLA de parches cerrados).                     |         |               |             |

Para más información contáctanos en nuestro sitio web **[www.certhia.pe](http://www.certhia.pe)**

## D) Operación y controles (muestra)

| Ítem                                                                           | Qué tener                                                                                                            | ✓ Listo | ⚠ En Progreso | ✗ Pendiente |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|---------|---------------|-------------|
| Gestión de identidades y accesos (altas/bajas/cambios, MFA, recertificaciones) | Proceso documentado, evidencia de bajas en ≤24h, MFA activo y recertificación periódica de privilegios.              |         |               |             |
| Gestión de privilegios y segregación de funciones                              | Lista de cuentas privilegiadas, justificación de acceso, segregación SoD y revisiones con correcciones.              |         |               |             |
| Vulnerabilidades y parches con SLA y cierres trazables                         | Herramienta de escaneo, criterios CVSS, SLA por criticidad, tickets de remediación con evidencia de despliegue.      |         |               |             |
| Copias de seguridad con pruebas de restauración                                | Política/cronograma de backups, registros de restauraciones exitosas, pruebas periódicas y responsables.             |         |               |             |
| Monitoreo y registros                                                          | Listado de fuentes (AD, EDR, firewalls, cloud), SIEM/alertas, retención definida y casos de uso con investigaciones. |         |               |             |

Para más información contáctanos en nuestro sitio web **[www.certhia.pe](http://www.certhia.pe)**

## E) Nube y proveedores

| Ítem                                                               | Qué tener                                                                                                      | ✓ Listo | ⚠ En Progreso | ✗ Pendiente |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|---------|---------------|-------------|
| Matriz de responsabilidad compartida (cloud) definida              | Matriz por servicio (IaaS/PaaS/SaaS) que delimite controles del proveedor vs. del cliente y evidencias.        |         |               |             |
| Configuración segura (plantillas aprobadas, 'hardening') y cifrado | Plantillas de configuración, informe de configuración segura, cifrado en tránsito/reposo y gestión de claves.  |         |               |             |
| Evaluación y clasificación de proveedores por criticidad           | Due diligence, criterios de criticidad, aprobación de onboarding y periodicidad de reevaluación.               |         |               |             |
| Contratos/SLAs con cláusulas de seguridad y auditoría              | Anexos con confidencialidad, ubicación de datos, respuesta a incidentes, subencargados, auditorías y métricas. |         |               |             |
| Monitoreo periódico del proveedor                                  | Informes (p. ej., SOC/ISO), KPIs de servicio, revisión periódica y evidencia de planes de mejora.              |         |               |             |

Para más información contáctanos en nuestro sitio web **[www.certhia.pe](http://www.certhia.pe)**

## F) Incidentes y continuidad

| Ítem                                                                   | Qué tener                                                                                                     | ✓ Listo | ⚠ En Progreso | ✗ Pendiente |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|---------|---------------|-------------|
| Gestión de incidentes (detección, respuesta, comunicación)             | Procedimiento con niveles de severidad, canales de comunicación, responsabilidades y registros de incidentes. |         |               |             |
| Revisión postincidente (lecciones aprendidas y análisis de causa raíz) | Acta de revisión, causas identificadas, acciones correctivas/preventivas y verificación de eficacia.          |         |               |             |
| Planes de continuidad/recuperación TIC probados                        | BCP/DRP con RTO/RPO, evidencias de ejercicios o simulacros y resultados.                                      |         |               |             |
| Resultados de pruebas y acciones de mejora registradas                 | Informe de prueba con hallazgos, responsables, plazos y seguimiento de acciones.                              |         |               |             |
| Integración de continuidad con riesgos y SoA                           | Actualización de matriz de riesgos y SoA tras pruebas/cambios relevantes de continuidad.                      |         |               |             |

Para más información contáctanos en nuestro sitio web **[www.certhia.pe](http://www.certhia.pe)**

## G) Privacidad y requisitos legales

| Ítem                                                       | Qué tener                                                                                                            | ✓ Listo | ⚠ En Progreso | ✗ Pendiente |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|---------|---------------|-------------|
| Inventario de tratamientos y base legal (si aplica)        | Registro de tratamientos, finalidades, bases legales, responsables y evaluaciones (p. ej., DPIA) cuando corresponda. |         |               |             |
| Controles de protección de datos integrados al SGSI        | Medidas técnicas/organizativas (minimización, cifrado, DLP, control de acceso) y evidencias de su operación.         |         |               |             |
| Matriz de requisitos legales/regulatorios actualizada      | Listado por país/sector (LOPDGDD/LPDP, cibersectoriales, etc.), responsables y evidencia de cumplimiento.            |         |               |             |
| Gestión de evidencias para auditorías/reguladores/clientes | Repositorio organizado, trazabilidad por requerimiento y procedimiento de respuesta a solicitudes.                   |         |               |             |

Para más información contáctanos en nuestro sitio web **[www.certhia.pe](http://www.certhia.pe)**

## H) Medición, auditoría interna y revisión por la dirección

| Ítem                                                               | Qué tener                                                                                                                 | ✓ Listo | ⚠ En Progreso | ✗ Pendiente |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|---------|---------------|-------------|
| Indicadores/KRI definidos, medidos y analizados                    | KPIs/KRIs con metas, periodicidad, tablero y decisiones tomadas a partir de los resultados.                               |         |               |             |
| Auditoría interna reciente con acciones y verificación de eficacia | Programa basado en riesgo, informes de auditoría, no conformidades/observaciones y cierre con verificación.               |         |               |             |
| Revisión por la dirección con entradas/salidas completas           | Acta con entradas (desempeño, incidentes, recursos, riesgos, cumplimiento) y salidas (decisiones y asignaciones).         |         |               |             |
| Gestión de cambios (6.3) activa y con trazabilidad                 | Registro de cambios relevantes, evaluación de impacto, aprobación, evidencias resultantes y actualización de riesgos/SoA. |         |               |             |

## I) Logística de auditoría

| Ítem                                                             | Qué tener                                                                                                       | ✓ Listo | ⚠ En Progreso | ✗ Pendiente |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|---------|---------------|-------------|
| Agenda, entrevistados y accesos a repositorios preparados        | Calendario por proceso/control, lista de entrevistados, accesos previos (read-only) y ambiente de demostración. |         |               |             |
| Evidencias etiquetadas (nomenclatura, ubicaciones, responsables) | Estructura de carpetas, nomenclatura consistente, responsables por evidencia y control de versiones.            |         |               |             |

Para más información contáctanos en nuestro sitio web **[www.certhia.pe](http://www.certhia.pe)**

Solicita información

[www.certhia.pe](http://www.certhia.pe)

CERTIFICACIONES  
**CERTHIA**  
VALIDAMOS TUS PASOS